UTILITY PATENT APPLICATION TRANSMITTAL

Address to:	*Attorney Docket No.*	FDC 0136 PUS
Box PATENT APPLICATION **Assistant Commissioner for Patents** **Washington, DC 20231**	*Inventor(s) or Application Identifier:* Julie A. Geschwender Michele Murphy-Houser	

1. This application entitled <u>"System and Method for Detecting Purchasing Card Fraud"</u> is:

   a. __X__ A new application under 37 C.F.R. §1.53(b).

   b. ____ A ____ continuation ____ divisional or ____ continuation-in-part application under 37 C.F.R. § 1.53(b) of prior application Serial No. ___/_____ filed on _____, entitled _____.

Application elements and other attached papers:

2. __X__ Specification (incl. Claims and Abstract)   [Total Pages <u>16</u>]

3. __X__ Drawings (___ informal <u>X</u> formal)   [Total Sheets <u>4</u>]

4. __X__ Oath or Declaration

   a. __X__ Newly-executed

   b. ____ Copy from a prior application (37 C.F.R. § 1.63(d))

5. ____ Incorporation By Reference: The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Item 4b, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.

6. ____ This application is filed by fewer than all the inventors named in the prior application, 37 C.F.R. § 1.53(d)(4).

   a. ____ *DELETE* the following inventor(s) named in the prior nonprovisional application:

   _____
   _____

   b. ____ The inventor(s) to be deleted are set forth on a separate sheet attached hereto.

CERTIFICATION UNDER 37 C.F.R. § 1.10

I hereby certify that this UTILITY PATENT APPLICATION TRANSMITTAL and the documents referred to as attached therein are being deposited on the below date with the United States Postal Service in an envelope as "Express Mail Post Office to Addressee" addressed to: Box Patent Application, Assistant Commissioner for Patents, Washington, D.C. 20231.

Express
Mail Label No. ___EJ124052685US___

Date of Deposit: ___October 22, 1999___

___Denise Sinnhuber___
(Type or print name of person mailing paper)

(Signature of person mailing paper)

7. Preliminary Amendment:

    a. ___ A Preliminary Amendment is attached.

    b. ___ Cancel in this application original claims _____ of the prior application before calculating the filing fee.

    c. ___ Please amend the specification by inserting before the first line the sentence:

        "This is a

        ___ continuation

        ___ divisional

        of copending application(s)

        ___ Serial number ___ /_____ filed on _____."

    d. ___ A Petition to Suspend Prosecution For The Time Necessary to File An Amendment (New Application Filed Concurrently) is attached.

8. Small entity status:

    a. ___ A small entity statement is attached.

    b. ___ A small entity statement was filed in the prior nonprovisional application and such status is still proper and desired.

    c. ___ Is no longer desired.

9. Fee Calculation:

FOR	NUMBER FILED	NUMBER EXTRA	RATE	CALCULATIONS
TOTAL CLAIMS (37 C.F.R. § 1 16(c))	26 -20 =	6	X 18.00	108.00
INDEPENDENT CLAIMS (37 C.F.R. § 1.16(b))	2 -3 =	0	X 78.00	0
MULTIPLE DEPENDENT CLAIMS (if applicable) (37 C.F.R. §1.16(d))		260.00		
			BASIC FEE (37 C F R. § 1 16(a))	760.00
		Total of above Calculations =		868.00
Reduction by 50% for filing by small entity (Note 37 C.F.R. §§ 1.9, 1.27, 1.28)				
		Assignment Recordal Fee	40.00	
			TOTAL =	868.00

10. _x_ A check in the amount of $ 868.00 is enclosed.

11. _x_ The Commissioner is hereby authorized to credit overpayments or charge the following fees (or any deficiency therein) to Deposit Account No. 02-3978 :

    a. _x_ Fees required under 37 C.F.R. § 1.16.

    b. _x_ Fees required under 37 C.F.R. § 1.17.

12. Maintenance of Copendency of Prior Application

___ A request for extension of time and the appropriate fee have been filed in the pending **prior** application (or are being filed in the prior application concurrently herewith) to extend the period for response until _____.

13. ___ An Information Disclosure Statement (IDS) is attached, along with the following indicated attachments thereto:

a. ___ Form PTO/SB/08 (_____ sheet(s))

b. ___ Copies of references cited

14. ___ Certified copy of priority document(s)

15. _X_ Return Receipt Postcard

16. ___ Other: _____
_____

17. ___ An Assignment of the invention to _____
_____

a. ___ is attached.

b. ___ was recorded on _____ at Reel _____, Frame _____.

18. The power of attorney in the prior application is to:

_____

Name of Attorney of Record   Reg. No.

___ The power appears in the original papers in the prior application.
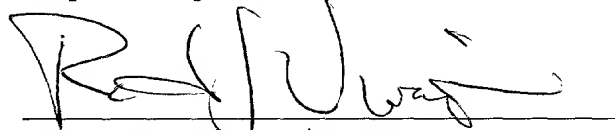
___ The power does not appear in the original papers, but was filed on _____.

___ A new power has been executed and is attached.

19. Correspondence Address: Please address all future communications to:

Paul M. Schwartz _____,
Brooks & Kushman P.C.,
1000 Town Center, 22nd Fl.
Southfield, MI 48075-1351
Telephone: 248-358-4400; Fax: 248-358-3351

Respectfully submitted,

Date _October 22, 1999_

Name: Raymond J. Vivacqua
Registration No.: P-45,369

_X_ Attorney or agent of record
___ Filed under Rule 34(a)

SYSTEM AND METHOD FOR
DETECTING PURCHASING CARD FRAUD

CROSS-REFERENCE TO RELATED APPLICATIONS

5   This application claims the benefit of U.S. Provisional Application No. 60/105,611, filed on October 26, 1998 and entitled "System and Method For Detecting Credit Card Fraud".

TECHNICAL FIELD

This invention relates to a system and method for detecting and
10   preventing purchasing card fraud during all phases of a purchasing card life cycle.

BACKGROUND ART

Roughly half a billion transactions with significant, but preventable, fraud potential occur in the United States each year. Purchasing card contact events that can lead to fraudulent occurrences include application processing, card
15   activation, usage, such as mail and phone ordering, and maintenance events, such as address or other information changes. It is estimated that the total cost of fraud is $1.3 million for every one million gross active accounts, or $1.34 in fraud loss per gross active account (Sources: VISA/MC, Credit Card Prevention Sourcebook).

A large portion of this fraud could effectively be addressed though
20   improved identification of known fraudulent names, fraudulent addresses, fraudulent phone numbers, fraudulent social security numbers, and other fraudulent personal information. In fact, a large number of fraud cases are typically perpetrated by repeat offenders or organized rings.

Current tools to combat repeat and organized fraud are still
25   underdeveloped. While there are a myriad of sources for fraud-related information,

the various sources focus on differing pieces of personal data and return fraudulent alerts in non-standard formats. In addition to the lack of uniformity of the alert information, current systems lack real time, "near" real time, or via batch functionality. Furthermore, no single comprehensive source exists that is capable

5   of addressing fraud during the many stages of a purchasing card account.

DISCLOSURE OF INVENTION

Therefore, it is an object of the present invention to provide a system and method for facilitating fraud prevention and detection at all stages of a purchasing card life cycle, wherein purchasing cards are defined as credit cards,

10   debit cards, "Smart" cards (having IC chips), retail cards (such as gas cards), and the like.

It is another object of the present invention to provide a single comprehensive database of standardized fraud data from various contributory sources.

15   It is still another object of the present invention to allow clients to reduce manual processes for fraud detection.

In accordance with these and other objects, the present invention provides a method and system for detecting purchasing card fraud during every aspect of a purchasing card life cycle. A central fraud database is created for

20   receiving known fraudulent or "high risk" personal information. The personal information may include, the fraudulent name, fraudulent addresses, fraudulent phone numbers, fraudulent places of employment, criminal history, and other personal information for example. The central fraud database receives information from a variety of sources including but not limited to proprietary databases, client

25   fraud files, law enforcement, and USPS databases. After a contact event has a occurred the fraud database is scanned for a match between the contact event information and the contents of the fraud database. If a possible fraud match occurs

the system sends a fraud alert to the client or user of the database. The present invention has many advantages over the prior art for example the present invention has the capability to send fraud alerts in real time, "near" real time, or via batch to clients thus reducing or eliminating the damage caused by potential purchasing card

5   fraud.

Thus in accordance with one aspect of the present invention, a method is provided for detecting purchasing card fraud during all phases of a purchasing card life cycle. The method includes obtaining contact event information from a client during a contact event, comparing the contact event information with

10   information stored in a database, and sending a fraud alert to a client in real time, "near" real time, or via batch for communicating to the client that a potential fraud match has occurred. Thus the method allows for special handling of the contact event by the client or user of the database.

In accordance with another aspect of the present invention, a system

15   for detecting purchasing card fraud during all phases of a purchasing card life cycle is provided. The system has a computer database for receiving contact event information from a client, computer software in communication with the computer database for comparing the contact event information with information stored in the database, and a communication network for sending a fraud alert to a client in real

20   time, "near" real time, or via batch for informing the client that a potential fraud match has occurred.

The above objects and other objects, features, and advantages of the present invention are readily apparent from the following detailed description of the best mode for carrying out the invention when taken in connection with the

25   accompanying drawings.

BRIEF DESCRIPTION OF DRAWINGS

FIGURE 1 is a schematic representation of a purchasing card fraud detection system designed in accordance with the present invention;

FIGURE 2 is a flow diagram of a preferred method of detecting purchasing card fraud in accordance with the present invention;

FIGURE 3 is a flow diagram of a preferred fraud matching process; and

FIGURE 4 is a schematic representation of a preferred fraud database architecture.

BEST MODE FOR CARRYING OUT THE INVENTION

The present invention provides a system and method for facilitating fraud prevention and detection for all contact events during a purchasing card life cycle. Such contact events include 1) application processing; 2) card activation; 3) cardholder usage, including mail and telephone orders; and 4) maintenance events, such as name and address changes, PIN changes, plastic requests, and credit line increases.

With reference to FIG. 1, the system of the present invention preferably includes a single, comprehensive risk database 10 for the detection of purchasing card fraud. The risk database 10 may include information from various sources 12, as will be described below. The risk database is preferably server-based and has connectivity, via a local area network 14 (LAN) or other network, to a mainframe 16. The mainframe 16 is provided for on-line transactions involving the various contact events 18 described above. Clients 20 are provided with connectivity to the risk database 10 for file transfer and general access, and are also provided connectivity to mainframe 16 (Graphical User Interface, dummy terminal or the like)

for receipt of fraud alerts and queue information. An optional, more limited database (not shown) could be provided for non-contributors to the risk database. Preferably, a backup server is provided.

The system of the present invention possesses the technical functionality to pool data from multiple sources in multiple formats and to standardize reporting structure guidelines, enabling the risk database to function for many types of transactions or contact events 18. In addition, the system provides the ability to query in real time, "near" real time, or via batch with on-line interfaces to the mainframe transactions. Preferably, limited client 20 resources are required for access.

In a preferred embodiment, at the mainframe 16 level, a daily queue statistics report is developed at the client 20 level to identify all accounts that match the risk database 10, including the source of the data match. Furthermore, at the server level, reports are generated which track contributor statistics. In addition, reporting is developed to track client statistics on a query basis, such as by the number of record transactions queried against the risk database 10, or by the number of records with a data match.

Possible sources for the consortium fraud database 10 include client databases, credit card issuer databases, credit bureau databases, research and investigation fraud files, ANI risk databases, the U.S. Postal Service NRI database, Account Takeover modeling/scoring, the Social Security Administration, the Department of Motor Vehicles, Western Union, Telecheck, the American Business List, law enforcement, court and public information records, phone directories, and direct mail surveys.

From such sources, the available data includes, but is not limited to, 1) personal information, such as addresses, phone numbers, and social security numbers used in known frauds; 2) valid US addresses and their nature, i.e. residential, commercial, or vacant; 3) valid address/name combinations; 4) high risk

zip codes; 5) public information, such as bankruptcy filings, tax liens, and civil judgments; and 6) consumer and purchase data.

The proposed data element structure within the risk database preferably includes at least the following:

1.   Names of fraudulent or potentially fraudulent ("high risk") primary, secondary, and additional cardholders in the form of first name, last name, and middle initial.

2.   Fraudulent or potentially fraudulent ("high risk") home and business addresses, including P.O. Box, city, state, and zip code.

3.   Fraudulent or potentially fraudulent ("high risk") home and business telephone numbers.

4.   Fraudulent or potentially fraudulent ("high risk") social security numbers of primary, secondary, and additional cardholders.

The risk database would act as a central repository for fraud data to be queried against by lenders and adjacent market users. Potential primary users or clients include bank card issuers, non-bank card issuers, potential card issuers, oil card issuers, merchants, and retailers. Possible secondary users include phone companies, DDA Account banks, and utility companies, among others.

The method of detecting potential purchasing card fraud of the present invention is outlined in the flow diagram of FIG. 2. The method includes obtaining contact event information at the mainframe 16, as represented by block 50. Comparing the contact event 18 information to fraud information stored in the risk database 10, as represented by block 52. If a match is found between the contact event information and the fraud information, the method further includes issuing an on-line alert to the client and queuing the information for manual review by the particular client, as represented by block 54. If a match does not occur client 20 is notified as such and communication with risk database 10 is concluded, as represented by block 56. Optionally, a fraud match may be scored, as represented by block 58 and as will be explained below. If a client 20 does not wish to receive a score then communication with the database is concluded, as represented by block

60. However, if a client has elected to receive a match score, a scorecard is generated and sent to the client 20, as represented by block 62 and then communication with risk database is terminated at block 64.

Within the system of the present invention, contact event 18 transactions are preferably structured to create automatic queries which compare account record data elements against the fraud information stored in the risk database. If a match is found between the account data and the fraud data, then an alert message is generated by the system in real time, "near" real time, or via batch to the queue. In addition, the account record is sent to an on-line queue to be monitored and/or manually worked by the client. Upon entry to the queue, the contact event transaction is suspended or placed on hold until manual follow-up is completed. The contact event information may for example be purged from the database.

An additional feature of the present invention is to offer clients 18 the option of having matched fraud data records "scored" to assist in the decisioning/actioning processes when a record is queued. Preferably, a generic suite of scorecards is provided, while also allowing client-defined scorecards to be developed and implemented. In a preferred embodiment, a scorecard is provided which predicts the likelihood of a fraudulent takeover of an existing, active, or inactive cardholder account.

The following attributes of the invention are thus possibly provided to facilitate fraud detection at all stages of a purchasing card life cycle:

- Application Processing
- Card Activation
- Cardholder Usage/Maintenance
- Other Transaction or Contact Events: Priority Non-Mons: PIN changes, plastic requests, credit line increases and changes to the account record.

The components of the invention are:

- Consortium Data Warehouse
- Fraud Scoring
- Actioning (Alerts to On-Line Screens)
- Queuing for Manual Review

The Matching Process

As shown in Figure 3, selected non-monetary transactions may be structured to create queries which compare account record data elements against the Consortium Risk Database 10 of the invention. For example, during an account entry transaction 80 (application processing, card activation, mail/phone order, address change, and the like) could automatically compare key application data elements against the Data Warehouse or Risk Database 10. If a match is found, as represented by block 82, between the account and the Data Warehouse, then an alert message 84 would be generated by the system real time, "near" real time, or via batch. In addition, the account record may be sent to an on-line queue 86 to be monitored and/or manually worked by the client. Upon entry to the queue, the non-monetary transactions would be suspended or placed on hold until manual follow up is completed. In the case of new account entries and batch-entered new accounts, the accounts may be built on the system, however, plastic generation would be suspended.

Information residing within the queue would include the account record information, the reason for the alert (i.e., potential fraudulent name, address, SSN, or phone number), and the contributing source of the matched data. This process will help to reduce responsibility/liability for data integrity.

Scoring of Matched Data

In further keeping with the invention, clients will be provided the option of having matched fraud data records "scored" to assist in the decisioning/actioning processes when a record is queued, as represented by block 88. This should provide business opportunities to build the appropriate scorecard logic.

-8-

Accordingly, a generic suite of scorecards 90 may be implemented as well as client-defined scorecards 92.

Consortium Contributors

5   All consortium contributors will be allowed access to the entire data warehouse. Usage incentives may also be provided for "global" contributors. An example of a usage incentive may be reduced fees for accessing the fraud database. Other incentives may include partial to full access to information contained in the fraud database.

10   ### Non-Consortium User

A non-contributor to the consortium may be offered access to information that the database manager may have purchased or provided in a non-consortium database 100. Otherwise non-contributors may be restricted from information provided by "global" contributors to the Risk Consortium Database.

15   ### Summary of Benefits and Critical Needs Met

- Provides a single source of uniform data from various contributor business sources;
- Increases the effectiveness of fraud detection efforts;
- Allows clients to reduce current manual processes for fraud
20   identification and actioning;
- Pools data across the client base to improve identification of repeat offenders.

Consortium Risk Data Warehouse

A consortium data warehouse contains data contributed from various
25   business sources 110 including, but not limited to:

- Clients;
- Research and Investigation Fraud Files (Fraud App's and Account takeovers (type lost 3,5,8));
- Customer Service Fraud File Database;

- Card Activation ANI Risk Database;
- Postal NRI Database (high risk Zip Codes);
- Social Security Administration compromised SSN's;
- International Association of Financial Crimes Investigators;
- Cellular or Pay Phone Numbers/Numbers used fraudulently;
- Western Union Fraud Data;
- American Business List (prison addresses, hospitals, etc.);
- Account takeover modeling/scoring;
- Potential model for Skimmin;
- American Correctional Association;
- Lexis/Nexis.

Proposed Data Element Structure

As depicted in Figure 4, the data element structure 200 may include:

- Name (Primary and Secondary and additional): First, Last, Middle Initial;
- Address: Home, Business (including PO Box);
- City;
- State;
- Zip Code;
- Phone: Home, Business;
- Social Security Number: Primary, Secondary;
- High Risk Zip Codes (NRI data); and
- Known fraudulent accounts determined by type lost.

Therefore, the system and method of the present invention provide a single source of uniform data from various contributor business sources 210, increase the effectiveness of fraud detection efforts, allow clients 212 to reduce current manual processes for fraud identification and actioning, and allow pooling of data across the client base to improve the identification of repeat offenders.

While embodiments of the invention have been illustrated and described, it is not intended that these embodiments illustrate and describe all possible forms of the invention. Rather, the words used in the specification are words of description rather than limitation, and it is understood that various changes

5   may be made without departing from the spirit and scope of the invention.

WHAT IS CLAIMED IS:

1   1.   A method for detecting purchasing card fraud during all phases

2 of a purchasing card life cycle, the method comprising:

3   obtaining contact event information from a client during a contact

4 event;

5   comparing the contact event information with information stored in

6 a database; and

7   sending a fraud alert to a client in real time for communicating to the

client that a fraud match has occurred.

1   2.   A method of claim 1 wherein obtaining contact event

2 information further comprises obtaining a customer's name, a customer's social

3 security number, customer's address, and a customer's fraud history.

1   3.   A method of claim 1 wherein comparing contact event

2 information with a fraud database further comprises comparing contact event

3 information with a fraud database having a plurality of fraud information sources.

1   4.   The method of claim 1 wherein obtaining contact event

2 information further comprises obtaining contact event information during a

3 purchasing card application process.

1   5.   The method of claim 1 wherein obtaining contact event

2 information further comprises obtaining contact event information during a

3 purchasing card activation process.

1   6.   The method of claim 1 wherein obtaining contact event

2   information further comprises obtaining contact event information during a

3   purchasing card mail order transaction from a retail participant.

1   7.   The method of claim 1 wherein obtaining contact event

2   information further comprises obtaining contact event information during a

3   purchasing card phone order transaction.

1   8.   A method of claim 1 wherein obtaining contact event

2   information further comprises obtaining contact event information during an address

3   change process.

1   9.   The method of claim 1 wherein sending an alert further

2   comprises sending an account record to an online queue to be monitored by the

3   client.

1   10.   The method of claim 9 wherein sending an account record

2   further comprises suspending the contact event until a manual follow-up is

3   completed.

1   11.   The method of claim 1 further comprising scoring the fraud

2   match to assist in the fraud determination process.

1   12.   The method of claim 11 wherein the scoring further comprises

2   predicting a likelihood of a fraudulent takeover of a cardholder account.

1   13.   The method of claim 1 further comprising suspending

2   purchasing card generation when a fraud match occurs.

3   14.   A system for detecting purchasing card fraud during all phases

4   of a purchasing card life cycle, the system comprising:

5   a computer database for receiving contact event information from a

6   client;

7   computer software in communication with the computer database for

8   comparing the contact event information with information stored in the database; and

9   a communication network for sending a fraud alert to a client in real

10   time for informing the client that a fraud match has occurred.

1   15.   A system of claim 14 wherein the contact event information

2   further comprises a customer's name, a customer's social security number,

3   customer's address, and a customer's fraud history.

1   16.   A system of claim 14 wherein the fraud database has a

2   plurality of fraud information sources.

1   17.   The system of claim 14 wherein the computer database

2   receives the contact event information during a purchasing card application process.

1   18.   The system of claim 14 wherein the computer database

2   receives the contact event information during a purchasing card activation process.

1   19.   The system of claim 14 wherein the computer database

2   receives the contact event information during a purchasing card mail order

3   transaction from a retail participant.

1   20.   The system of claim 14 wherein the computer database

2 receives the contact event information during a purchasing card phone order

3 transaction.

       21.   The system of claim 14 wherein the computer database receives the contact event information during an address change process.

1   22.   The system of claim 14 wherein the fraud alert is an account

2 record which is sent to an online queue monitored by a client.

1   23.   The system of claim 22 wherein sending an account record

2 further comprises suspending the contact event until a manual follow-up is

3 completed.

1   24.   The system of claim 14 further comprising scoring the fraud

2 match to assist in the fraud determination process.

1   25.   The system of claim 24 wherein the scoring the fraud match

2 further comprises predicting a likelihood of a fraudulent takeover of a cardholder

3 account.

4   26.   The system of claim 14 wherein purchasing card generation

5 is suspended when a fraud match occurs.

ABSTRACT OF THE DISCLOSURE

A method and system for detecting purchasing card fraud during every aspect of a purchasing card life cycle is disclosed. A central fraud database is created for receiving potential fraud or "high risk" information. The fraudulent

5   information may include, fraudulent customer names, addresses, phone numbers, places of employment, criminal histories, and other personal information. The central fraud database receives information from a variety of sources including but not limited to client fraud files, law enforcement files, and USPS databases. After a contact event has a occurred the fraud database is scanned for a match between the

10   contact event information and the contents of the fraud database. If a fraud match occurs the system sends a fraud alert to the client, including a scorecard. The client is given options to respond to the contact event, such as suspending purchasing card generation.

CONTRACT EVENT 1   CONTRACT EVENT 2   CONTRACT EVENT 3   CONTRACT EVENT n

18

14

14

16   MAINFRAME   CLIENT 1

14   14

SOURCE 1   CLIENT 2

SOURCE 2   20

SOURCE 3   RISK   CLIENT n
           DATABASE

12 SOURCE 4   10

SOURCE 5

SOURCE n

Fig. 1

START

50 — OBTAIN CONTACT
EVENT INFORMATION

FRAUD MATCH WITH
DATABASE INFORMATION
?

52

NO → END

56

YES

54 — SEND ALERT AND
QUEUE FOR CLIENT PROCESSING

SCORE
?

58

NO → END

60

YES

62 — GENERATE
SCORECARDS(S)

64 — END

Fig. 2

18

APPLICATION
PROCESSING

CARD
ACTIVATION

MAIL/PHONE
ORDER

ADDRESS
CHANGE

ON-LINE
TRANSACTIONS

CUSTOMER
SERVICE
FRAUD

RESEARCH &
INVESTIGATION
FRAUD FILE

POSTAL
INFORMATION

110

SOCIAL
SECURITY
ADMINISTRATION

CLIENT

CLIENT

CONSORTIUM
FRAUD
DATABASE

10

82

88

FRAUD
MATCH
?

YES

SCORE
?

NO

NO

YES

END

OTHER
SCORECARD

90

ATO
SCORECARD

92

CUSTOM
CLIENT
SCORECARD

CLIENT

FRAUD
FILE

NON-
CONSORTIUM
DATABASE

100

84

ON-LINE
ALERT

86

QUEUE

Fig. 3

210

- CLIENT FRAUD FILES
- DQI²
- SHARE FORCE
- FALCON QUEUE
- LAW ENFORCEMENT
- USPS DATABASES
- OTHER EXTERNAL DATABASES

200

Name:	Doug Wilson
SSN:	123-45-6789
Address:	5 Fraud Dr. Omaha, NE 12345
Type:	Commercial Receipt
Home Phone:	(402) 555-5555
Business Phone:	(402) 777-7777
History:	Convicted Fraud
Date:	1/3/95

Record #00197362415
Record #00264178320
Record #00147892310
Record #00423714765

212

- BANK CARD ISSUERS
- NON-BANK CARD ISSUERS
- POTENTIAL CARD ISSUERS
- OIL CARD ISSUERS
- MERCHANTS
- PHONE COMPANIES
- DDA ACCOUNT BANKS
- UTILITY/TELEPHONE
- OTHER

Fig. 4

DECLARATION FOR PATENT APPLICATION AND POWER OF ATTORNEY

Atty. Docket No. __FDC 0112 PUS__

First Named Inventor __Julie A. Geschwender et al.__

As a below named inventor, I hereby declare that my residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

SYSTEM AND METHOD FOR DETECTING PURCHASING CARD FRAUD ,

the specification of which:

[x] is attached hereto; or

[ ] was filed on (MM/DD/YYYY) ___ as U.S. Application Number or PCT International Application Number _____, and was amended on (MM/DD/YYYY) ___ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment specifically referred to above.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, §1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, § 119(a)-(d) or § 365(b) of any foreign application(s) for patent or inventor's certificate, or § 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below, and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or of any PCT international application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application Number(s)	Country	Foreign Priority Date (MM/DD/YYYY)	Priority Not Claimed	Certified Copy Attached? (Yes/No)

I hereby claim the benefit under Title 35, United States Code, § 119(e) of any United States provisional application(s) listed below.

Application Number(s)	Filing Date (MM/DD/YYYY)
60/105.611	October 26, 1998

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code § 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, § 1.56 which occurred between the filing date of the prior application and the national or PCT international filing date of this application.

Application Number(s)	Filing Date (MM/DD/YYYY)	Status: Patented, Pending, Abandoned

B&K0001/9801

[Decl. -- Page 1 of 2]

Declaration for Patent Application (cont'd.)   Atty. Docket No. _____

I hereby appoint the following registered practitioners to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith:

Ernie L. Brooks, Reg. No. 26,260; James A. Kushman, Reg. No. 25,634; David R. Syrowik, Reg. No. 27,956; Mark A. Cantor, Reg. No. 30,614; Ralph M. Burton, Reg. No. 17,748; Robert C.J. Tuttle, Reg. No. 27,962; Earl J. LaFontaine, Reg. No. 30,766; Ronald M. Nabozny, Reg. No. 28,648; Thomas A. Lewry, Reg. No. 30,770; John E. Nemazi, Reg. No. 30,876; Kevin J. Heinl, Reg. No. 29,805; William G. Abbatt, Reg. No. 31,936; Donald J. Harrington, Reg. No. 17,427; Paul M. Schwartz, Reg. No. 33,278; Timothy G. Newman, Reg. No. 34,228; Frederick M. Ritchie, Reg. No. 18,669; Robert C. Brandenburg, Reg. No. 29,048; A. Frank Duke, Reg. No. 20,937; John M. Halan, Reg. No. 35,534; Jeffrey M. Szuma, Reg. No. 35,700; James R. Ignatowski, Reg. No. 26,741; Frank A. Angileri, Reg. No. 36,733; William G. Conger, Reg. No. 31,209; Sangeeta G. Shah, Reg No. 38,614; Christopher W. Quinn, Reg. No. 38,274; Robert C. Jones, Reg. No. 35,209; David S. Bir, Reg. No. 38,383; Konstantine J. Diamond, Reg. No. 39,657; James N. Kallis, Reg. No. 41,102; Hugo A. Delevic, Reg. No. 32,688; Ralph E. Smith, Reg. No. 35,474; Michael S. Brodbine, Reg. No. 38,392; Jeremy J. Curcuri, Reg. No. 42,454; Mark D. Chuey, Reg. No. 42,415; and John J. Ignatowski, Reg. No. 36,555; Pete N. Kiousis, Reg. No. 41,117; Gigette M. Bejin, Reg. No. 44,027; Stephanie M. Mansfield, Reg. No. 43,773; Mark E. Stuenkel, Reg. No. 44,364, Matthew R. Mowers, Reg. No. P-44,956; Raymond J. Vivacqua, Reg. No. P-45,369.

Address all correspondence and telephone calls to ___Paul M. Schwartz_____
at Brooks & Kushman P.C., 1000 Town Center, Twenty-Second Floor, Southfield, Michigan 48075, (248) 358-4400.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of Sole or First Inventor ___Julie A. Geschwender_____

Inventor's signature _____ Date __10/22/99__

Post Office Address ___SAME AS RESIDENCE_____

Residence ___711 N. 89 Plaza, Omaha, Nebraska 68114_____ Citizenship ___U.S.A.___

Full Name of Second Joint Inventor ___Michelle Murphy-Houser_____

Inventor's signature _____ Date _____

Post Office Address ___SAME AS RESIDENCE_____

Residence ___3355 S. 114th Avenue, Omaha, Nebraska 68144_____ Citizenship ___U.S.A.___

Full Name of Third Joint Inventor _____

Inventor's signature _____ Date _____

Post Office Address _____

Residence _____ Citizenship _____

Full Name of Fourth Joint Inventor _____

Inventor's signature _____ Date _____

Post Office Address _____

Residence _____ Citizenship _____
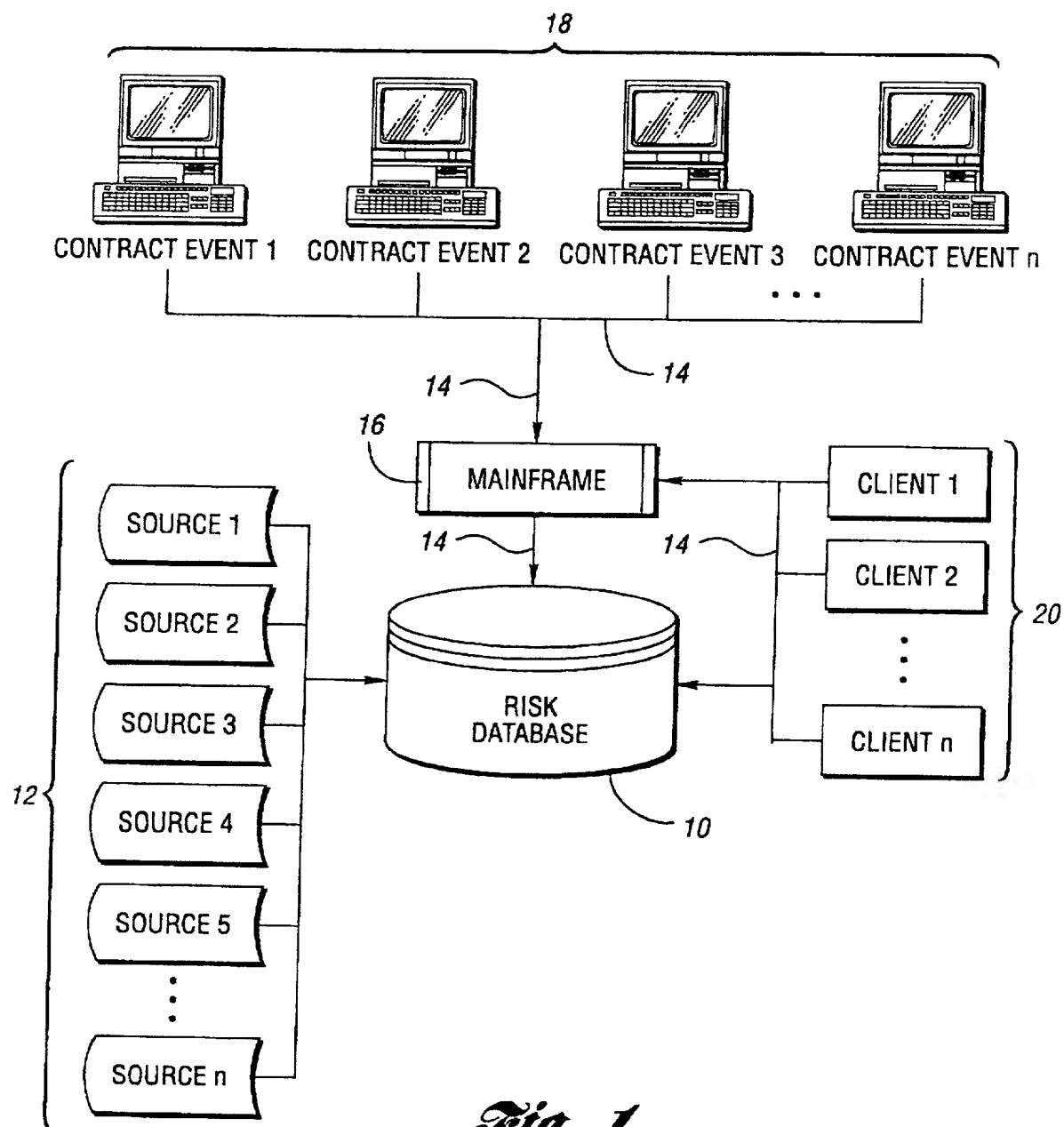
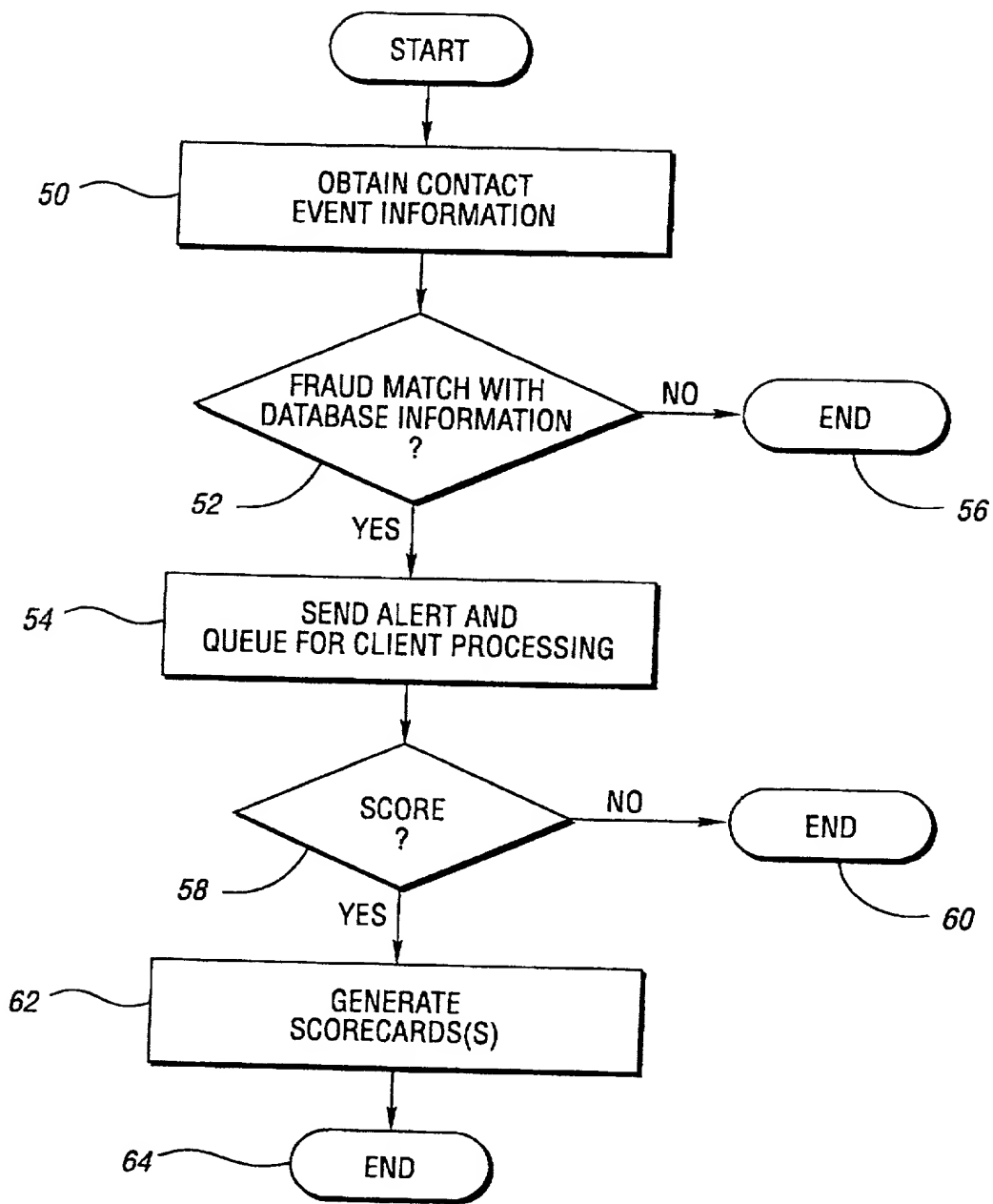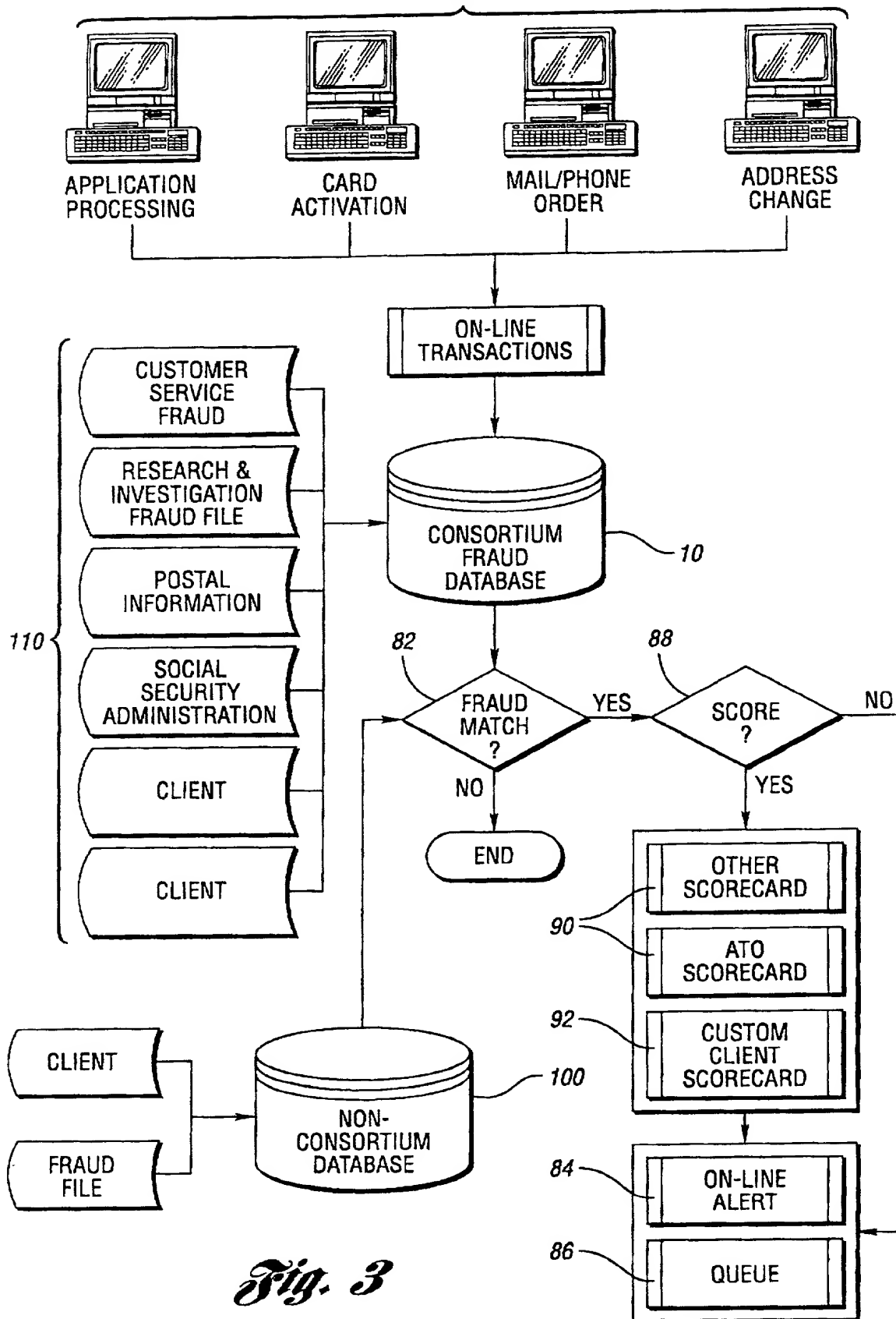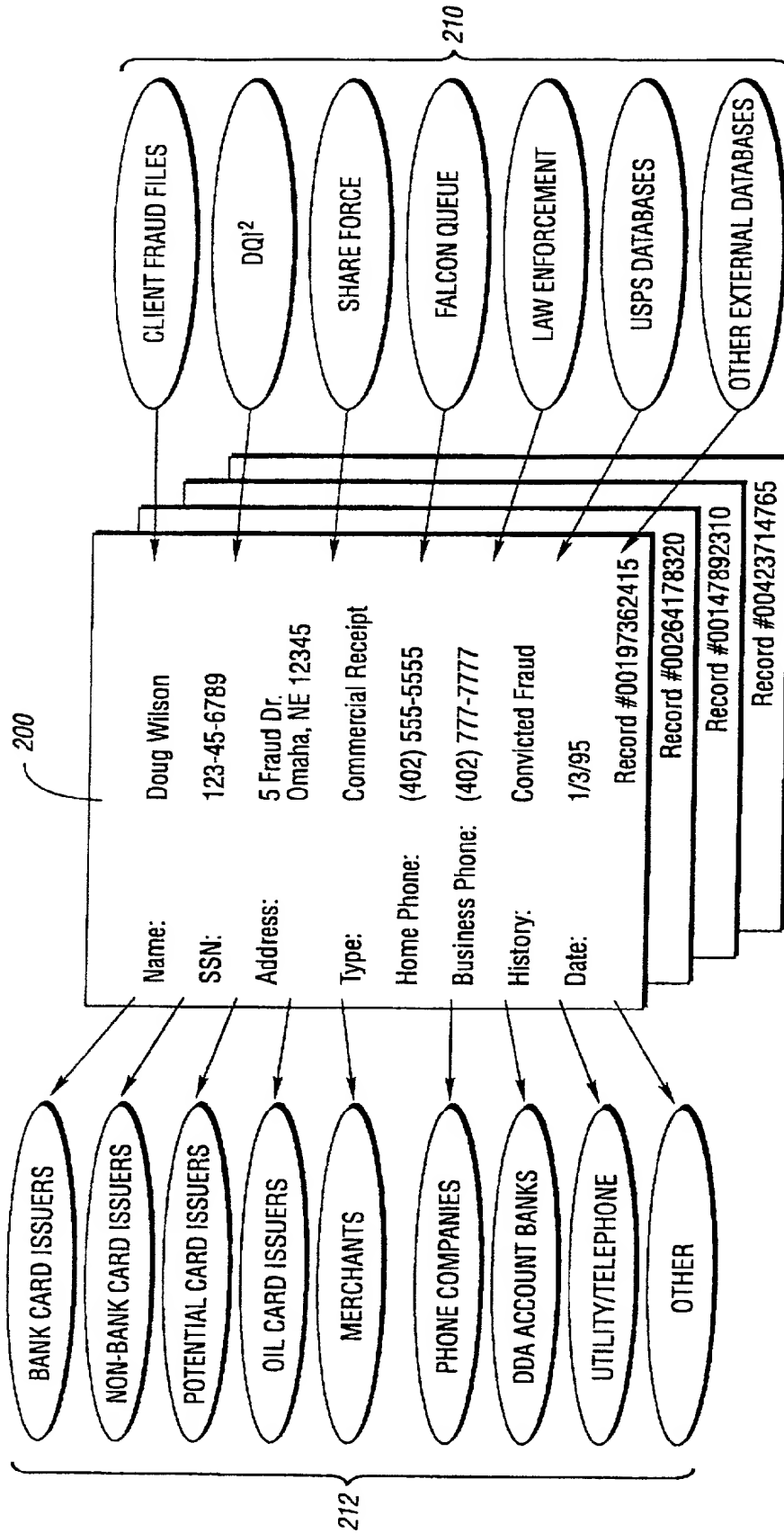B&K0001/9801   [Decl. – Page 2 of 2]

DECLARATION FOR PATENT APPLICATION AND POWER OF ATTORNEY

Atty. Docket No. ___FDC 0136 PUS_____

First Named Inventor __Julie A. Geschwender et al._____

As a below named inventor, I hereby declare that my residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

SYSTEM AND METHOD FOR DETECTING PURCHASING CARD FRAUD ,

the specification of which:

[x] is attached hereto; or

[   ] was filed on (MM/DD/YYYY) ____ as U.S. Application Number or PCT International Application Number _____, and was amended on (MM/DD/YYYY) ____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment specifically referred to above.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, §1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, § 119(a)-(d) or § 365(b) of any foreign application(s) for patent or inventor' certificate, or § 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below, and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or of any PCT international application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application Number(s)	Country	Foreign Priority Date (MM/DD/YYYY)	Priority Not Claimed	Certified Copy Attached? (Yes/No)

I hereby claim the benefit under Title 35, United States Code, § 119(e) of any United States provisional application(s) listed below.

Application Number(s)	Filing Date (MM/DD/YYYY)
60/105,611	October 26, 1998

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code § 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, § 1.56 which occurred between the filing date of the prior application and the national or PCT international filing date of this application.

Application Number(s)	Filing Date (MM/DD/YYYY)	Status: Patented, Pending, Abandoned

B&K0001/9801   [Decl. -- Page 1 of 2]

Declaration for Patent Application (cont'd.)   Atty. Docket No. __FDC 0136 PUS__

I hereby appoint the following registered practitioners to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith:

Ernie L. Brooks, Reg. No. 26,260; James A. Kushman, Reg. No. 25,634; David R. Syrowik, Reg. No. 27,956; Mark A. Cantor, Reg. No. 30,614; Ralph M. Burton, Reg. No. 17,748; Robert C.J. Tuttle, Reg. No. 27,962; Earl J. LaFontaine, Reg. No. 30,766; Ronald M. Nabozny, Reg. No. 28,648; Thomas A. Lewry, Reg. No. 30,770; John E. Nemazi, Reg. No. 30,876; Kevin J. Heinl, Reg. No. 29,805; William O. Abbatt, Reg. No. 31,936; Donald J. Harrington, Reg. No. 17,427; Paul M. Schwartz, Reg. No. 33,278; Timothy G. Newman, Reg. No. 34,228; Frederick M. Ritchie, Reg. No. 18,669; Robert C. Brandenburg, Reg. No 29,048; A. Frank Duke, Reg. No. 20,937; John M. Hulan, Reg. No. 35,534; Jeffrey M. Szuma, Reg. No. 35,700; James R. Ignatowski, Reg. No. 26,741; Frank A. Angileri, Reg. No. 36,733; William T. Conger, Reg. No. 31,209; Sangeeta G. Shah, Reg. No. 38,614; Christopher W. Quinn, Reg. No. 38,274; Robert C. Jones, Reg. No. 35,209; David S. Bir, Reg. No. 38,383; Konstantine J. Diamond, Reg. No. 39,657; James N. Kallis, Reg. No. 41,102; Hugo A. De Vie, Reg. No. 32,688; Ralph E. Smith, Reg. No. 35,174; Michael S. Brodbine, Reg. No. 39,392; Jeremy J. Curcuri, Reg. No. 43,454; Mark D. Chuey, Reg. No. 42,415; and John J. Ignatowski, Reg. No. 36,555; Pete N. Kiousis, Reg. No. 41,117; Gigette M. Bejin, Reg. No. 44,027; Stephanie M. Mansfield, Reg. No. 43,773; Mark E. Stuenkel, Reg. No. 44,364; Matthew R. Mowers, Reg. No. P-44,956; Raymond J. Vivacqua, Reg. No. P-45,369.

Address all correspondence and telephone calls to __Paul M. Schwartz__
at Brooks & Kushman P.C., 1000 Town Center, Twenty-Second Floor, Southfield, Michigan 48075, (248) 358-4400.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of Sole or First Inventor __Julie A. Geschwender__

Inventor's signature __SEE OTHER DOCUMENT__   Date _____

Post Office Address __SAME AS RESIDENCE__

Residence __711 N. 89 Plaza, Omaha, Nebraska 68114__   Citizenship __U.S.A.__

Full Name of Second Joint Inventor __Michelle Murphy-Houser__ MMH

Inventor's signature _____   Date __10/22/99__

Post Office Address __SAME AS RESIDENCE__

Residence __3355 S. 114th Avenue, Omaha, Nebraska 68144__   Citizenship __U.S.A.__

Full Name of Third Joint Inventor _____

Inventor's signature _____   Date _____

Post Office Address _____

Residence _____   Citizenship _____

Full Name of Fourth Joint Inventor _____

Inventor's signature _____   Date _____

Post Office Address _____

Residence _____   Citizenship _____